(1) **V závislosti na $k \in \mathbb{N}$ určete největšího společného dělitele čísel $2k-1$ a $3k+1$.**

**Řešení.** Použijeme odečítací verzi Eukleidova algoritmu, tj. fakt, že platí

$$NSD(a,b) = NSD(b, a-b)$$

Tedy platí následující posloupnost rovností:

$$\begin{aligned} NSD(3k+1, 2k-1) &= NSD(2k-1, k+2) \\ &= NSD(k+2, 5) \end{aligned}$$

Tedy vidíme, že největší společný dělitel může být jedině 1 nebo 5.

$$NSD(2k-1, 3k+1) = \begin{cases} 5 & \text{pokud } 5 \mid k+2 \\ 1 & \text{jinak} \end{cases}$$

(2) **Pro polynomy $p = 4x^4 + 6x^3 + x^2 + 1$, $q = x^2 + 4x + 3$ najděte polynomy $r$, $s$, aby $rp + sq$ byl roven (nějakému) největšímu společnému děliteli $p$, $q$. (Všechny operace provádějte nad tělesem racionálních čísel.)**

**Řešení.** Danou rovnost splnují Bézoutovy koeficienty $r$ a $s$, které dostaneme jako výstup rozšířeného Eukleidova algoritmu. Tabulka výpočtu vypadá následovně:

| | | |
|---|---|---|
| $p$ | 1 | 0 |
| $q$ | 0 | 1 |
| $-86(x+1)$ | 1 | $-4x^2 + 10x - 29$ |
| 0 | | |

Polynom $-86(x+1)$ dělí polynom $q$, je tedy největším společným dělitelem polynomů $p$, $q$ a platí

$$NSD(p,q) = -86(x+1) = \underbrace{1}_{r} \cdot p + \underbrace{(-4x^2 + 10x - 29)}_{s} \cdot q$$

(3) **Určete poslední cifru čísla $2^{2012} - 1$.**

**Řešení.** Poslední cifra čísla $2^{2012}-1$ je rovna číslu $2^{2012}-1 mod 10$. Pokusným mocněním snadno zjistíme, že platí

$$2^k \equiv 2^{k+4} \ (mod\, 10) \quad \text{pro } k \in \mathbb{N} - \{0\}$$

Protože $2012 \equiv 4 \ (mod\, 4)$, platí

$$2^{2012} - 1 \equiv 2^4 - 1 \equiv 5 \quad (mod\, 10)$$

Tedy poslední cifra čísla $2^{2012} - 1$ je 5.

(4) **Vyřešte v celých číslech rovnici $x^2 + 10x + 6 \equiv 0 \ (mod\, 17)$ .**

**Řešení.** Počítáme modulo 17, původní rovnici tedy můžeme přepsat jako

$$\begin{aligned} x^2 + 10x + 6 &\equiv 0 \quad (mod\, 17) \\ x^2 + 10x - 11 &\equiv 0 \quad (mod\, 17) \\ (x-1)(x+11) &\equiv 0 \quad (mod\, 17) \end{aligned}$$

Podle lemmatu "$p|ab \Rightarrow p|a$ nebo $p|b$" tedy platí:

$$\begin{aligned} x - 1 &\equiv 0 \quad (mod\, 17) \\ x &\equiv 1 \quad (mod\, 17) \end{aligned}$$

nebo

$$\begin{aligned} x + 11 &\equiv 0 \quad (mod\, 17) \\ x &\equiv 6 \quad (mod\, 17) \end{aligned}$$

Množina řešení rovnice je tedy:

$$x \in \{1 + 17k,\ 6 + 17k\ :\ k \in \mathbb{Z}\}$$